Raspodijeljene glavne knjige i kriptovalute

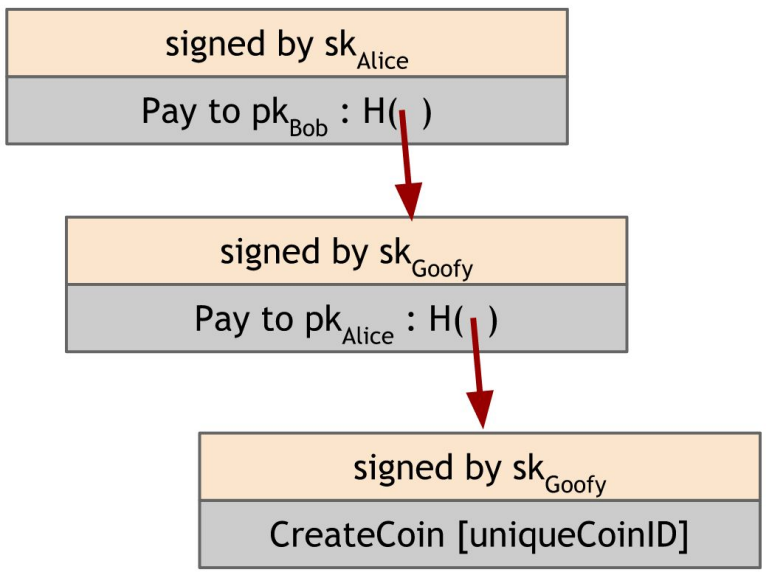
Nakamotov konsenzus

Ante Đerek, Zvonko Konstanjčar

22. listopada 2021.

Stvaranje i prenošenje novčića

- Samo Željko može stvarati novčiće.
- *Vlasnik* novčića može ga prenijeti nekome drugome.

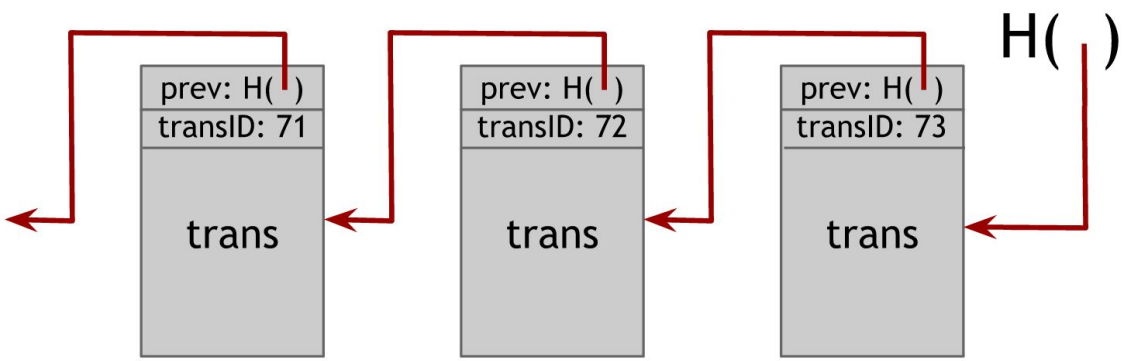


Izvor: `bitcoinbook.cs.princeton.edu`

transID: 73	type:CreateCoins	
coins created		
num	*value*	*recipient*
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...

coinID 73(0)
coinID 73(1)
coinID 73(2)

transID: 73	type:PayCoins	
consumed coinIDs: 68(1), 42(0), 72(3)		
coins created		
num	*value*	*recipient*
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...
signatures		



Izvor: bitcoinbook.cs.princeton.edu

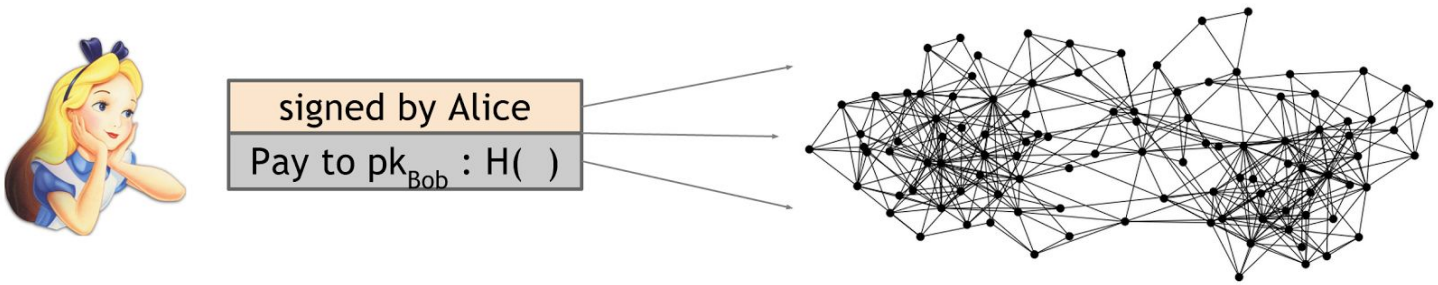
Branko bilježi transakciju tako da:

1. Provjeri da novčić c nije već potrošen.
2. Provjeri da iznos novog novčića odgovara iznosu novčića c.
3. Provjeri da je c stvarno novčić koji pripada Ani.
4. Provjeri ispravnost potpisa na transakciji pomoću Aninog javnog ključa.
5. Dodaje transakciju u lanac blokova.

```
transaction:
  type: CreateCoins
  consumedCoinId: 73(0)
  coinsCreated:
    - value: 3.2
      recipient: 0xe7a0f06858dc8a2323e387cbe797cf48...
signature: 0xc9491ba77e2e8a19040826f0e070162d...
```

Arhitektura sustava

- Puno čvorova u "peer-to-peer" mreži.
- Svi čvorovi imaju identične kopije lanca blokova.
- Svaki čvor održava skup transakcija koje treba dodati u lanac.
- Periodički se dodaje novi blok u lanac:
  - Svaki čvor predloži potencijalni sljedeći blok.
  - Čvorovi se nekako usaglase čiji će prijedlog dodati u lanac.
  - Svaki čvor doda odabrani blok u svoj lanac.

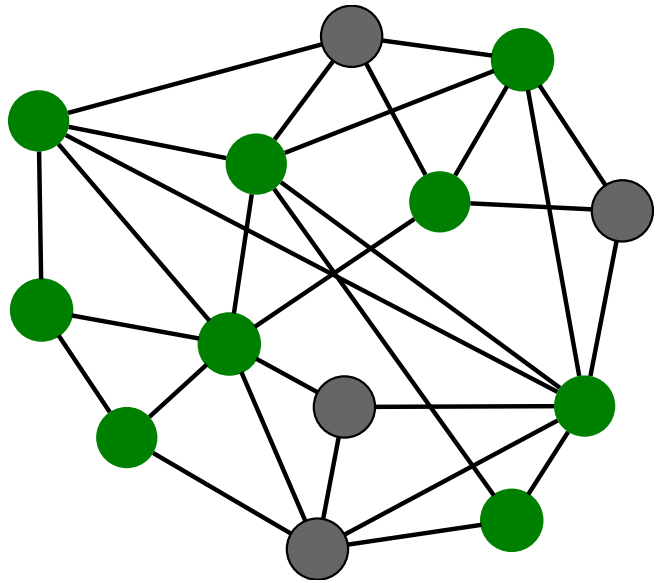


Izvor: `bitcoinbook.cs.princeton.edu`

Definicija

U mreži se nalazi n čvorova, neki čvorovi su ispravni i oni vjerno prate pravila protokola, dok su drugi neispravni ili zlonamjerni. Svaki čvor k ima neku ulaznu vrijednost x_k. Protokol za raspodijeljeni konsenzus je mehanizam za kojeg vrijedi:

- *Svaki ispravni čvor k izračuna izlaznu vrijednost y_k.*
- *Izlazna vrijednost svih ispravnih čvorova je jednaka.*
- *Ta izlazna vrijednost je jednaka ulaznoj vrijednosti x_k nekog ispravnog čvora.*

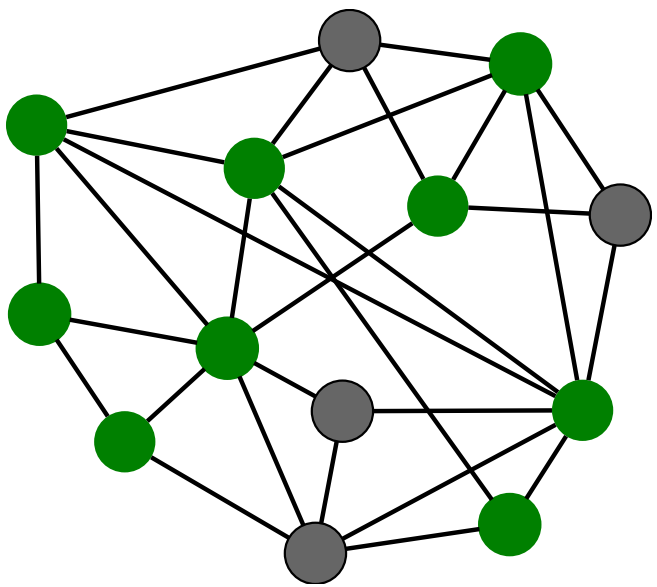


Težak problem

- Teorijski rezultati: nemoguće ako je komunikacija asinkrona, nemoguće ako je više od jedne trećine čvorova zlonamjerno.
- "Standardno" rješenje: Paxos protokol.
- Bitcoin: "Proof-of-work"

Nerealna pretpostavka

Postoji mehanizam (nazovimo ga "KBV") koji omogućuje odabir slučajnog čvora u mreži. Štoviše, mehanizam je takav da je vjerojatnost da je slučajno odabrani čvor *ispravan* veća od pola.



Postupak određivanja sljedećeg bloka

- KBV odabere slučajni čvor A i objavi ga svim čvorovima.
- A predloži sljedeći blok x i objavi ga svim čvorovima.
- Ostali čvorovi provjeravaju ispravnost bloka x.
- Čvorovi *prihvaćaju* blok x ako je ispravan, ignoriraju ako nije.

Pažnja!

- Blok sadrži hash pokazivač na prethodni blok. Dakle, prihvaćanje bloka je *prihvaćanje lanca*, provjera ispravnosti bloka je *provjera ispravnosti lanca*.
- Konsenzus je *implicitan* – ako je čvor prihvatio novi blok onda će njega nadograđivati ako njega sljedećeg odabere KBV.

Zadatak

Kako korisnik zna koji je lanac "pravi"?

Zadatak

Može li napadač ukrasti ili potrošiti tuđi novčić?

Zadatak

Može li napadač uskratiti uslugu određenom korisniku?

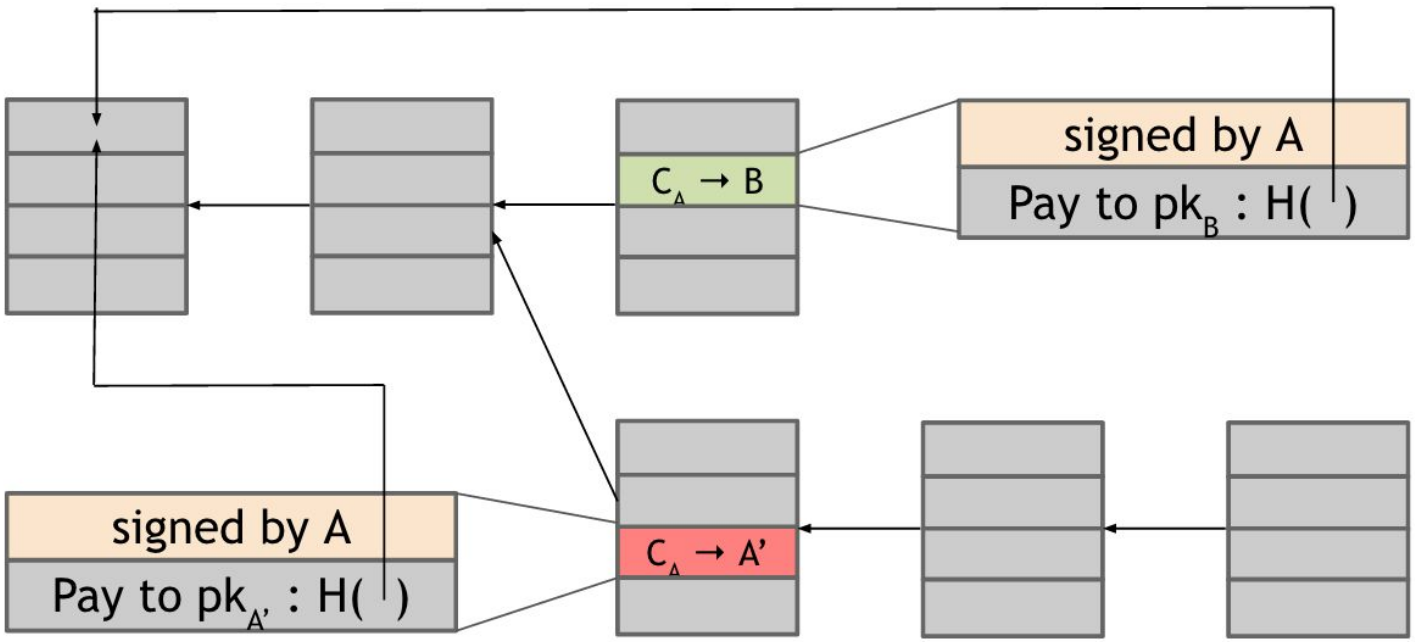
Zadatak

Može li napadač vlastiti novčić potrošiti dvaput?

Napad

1. Ana izradi i objavi transakciju t kojom šalje novčić c Branku.
2. Transakciju t čvor kojeg je odabrala KBV uključi u blok.
3. Branko pošalje Ani plaćenu robu.
4. U sljedećem koraku KBV odabere Anu.
5. Ana objavi blok koji se veže na predzadnji blok u lancu

Pojednostavljeni Nak. kon. – dvostruko trošenje



Izvor: `bitcoinbook.cs.princeton.edu`

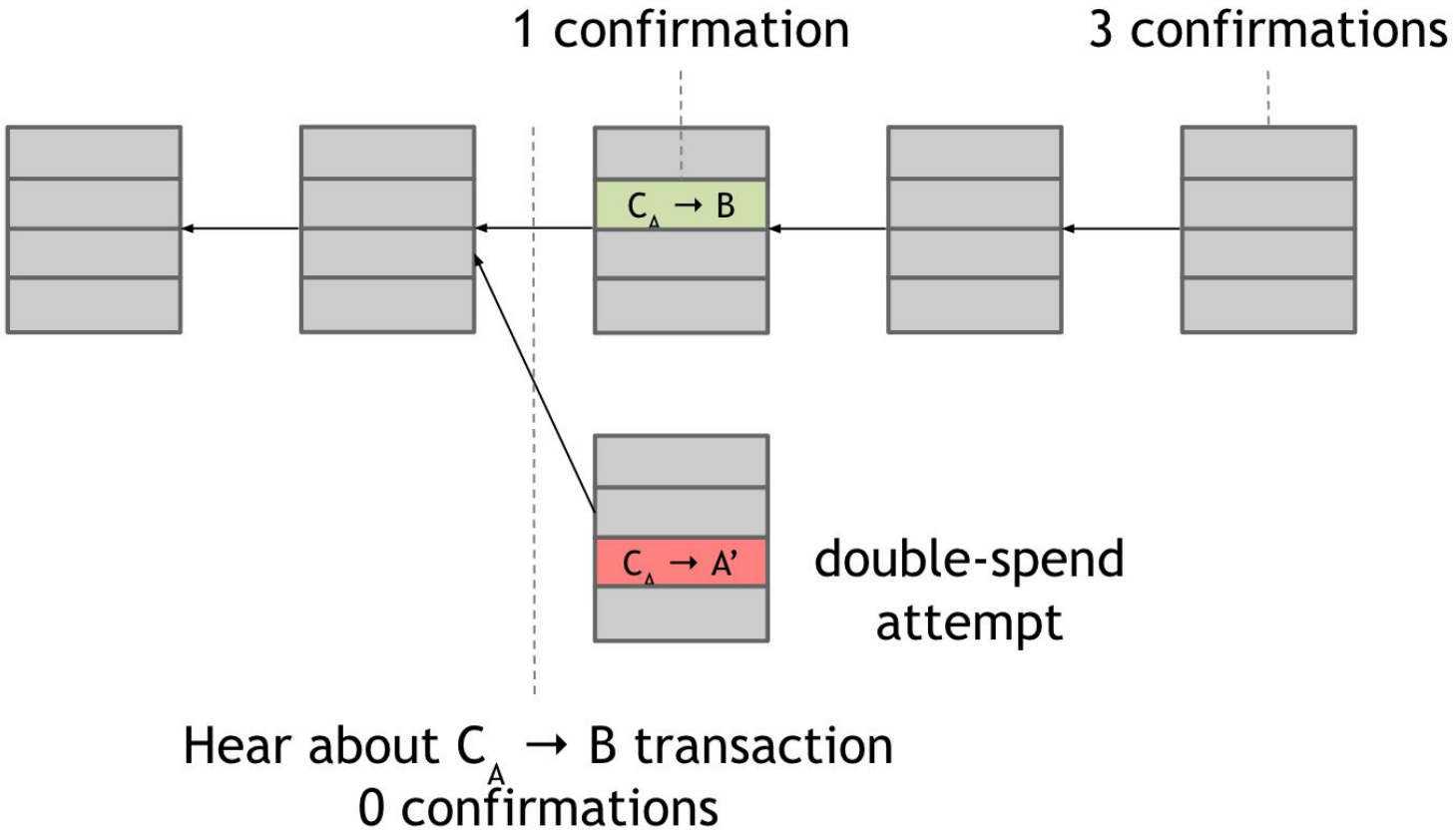
Novo pravilo: najduži lanac

Čvorovi uvijek produžuju *najduži* ispravni lanac za kojeg znaju. Drugim riječima, čvor prihavaća novi lanac samo ako je ispravan i ima više blokova od trenutnog lanaca tog čvora.

Zadatak

Pomaže li ovo pravilo Branku da se obrani protiv napada?

Pojednostavljeni Nak. kon. – dvostruko trošenje



Izvor: `bitcoinbook.cs.princeton.edu`

Sažetak

- Kriptografija štiti od krađe i neispravnih transakcija.
- Konsenzus štiti od dvostrukog trošenja, ali samo ako je primatelj oprezan.
- Konsenzus je implicitan.
- Konsenzus je vjerojatnosni.
- Konsenzus se zasniva na nerealnom mehanizmu KBV.

Gdje je lova?

Imate onoliko novaca koliko konsenzus u mreži kaže da imate.

Cilj: Potaknuti čvorove na ispravno ponašanje

- Možemo li nekako "kazniti" čvor koji je pokušao dodati transakciju koja troši novčić dvaput?
- Možemo li nekako "nagraditi" čvor čiji blok dugoročno završi u lancu blokova?

Mehanizmi nagrade

- Nagrada za blok.
- Naknada za transakciju.

Novo pravilo: nagrada za blok

Čvor koji predlaže novi blok može u njega uključiti jednu posebnu transakciju kojom nastaje novi novčić.

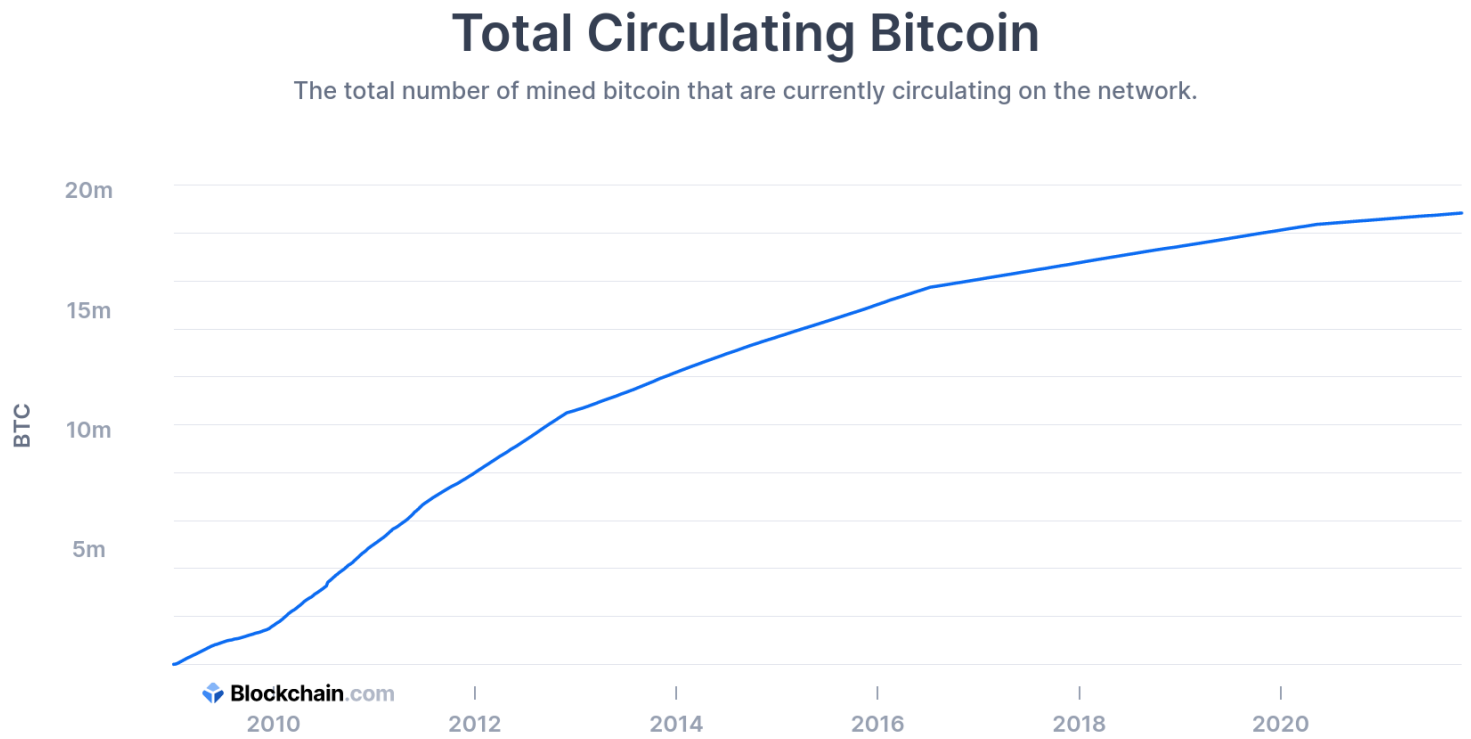
```
transaction:
  type: CreateCoins
  coinsCreated:
    - value: 12.5
      recipient: 0xe7a0f06858dc8a2323e387cbe797cf48...
```

Poticaj!

U financijskom interesu čvora koji predlaže novi blok je da taj blok bude uključen u lanac oko kojeg će nastati konsenzus.

Detalji nagrade za blok u sustavu Bitcoin (listopad 2021.)

- Jedini mehanizam kojim nastaju novi BTC-i!
- Vrijednost nagrade je trenutno 6.25 BTC ($400,000).
- Vrijednost nagrade se prepolovi svakih 210,000 blokova.
- Nagrada se može potrošiti tek nakon 100 blokova.



Novo pravilo: naknada za transakciju

- Zbroj vrijednosti novčića koji se troše mora biti *veći ili jednak* od zbroja vrijednost novčića koji nastaju.
- Razlika se naziva *naknada za transakciju*.
- Sve naknade za transakcije se pribrajaju nagradi za blok.

Poticaj!

U financijskom interesu čvora koji predlaže novi blok je da taj blok uključuje što više ispravnih transakcija.

Što točno znači kada kažemo “novo pravilo”?

Pravila konsensusa

Sva navedena pravila se implementiraju tako da se promijeni definicija *ispravnosti bloka odnosno lanca*. Prije prihvaćanja novog bloka (odnosno lanca) svaki čvor između ostalg provjerava:

- Jesu li ispravno izračunate naknade za transakcije.
- Je li ispravno izračunata nagrada za blok.
- Je li nagrada za blok prerano potrošena.
- ...

Pravila konsensusa

Pravila su implementirana *unutar* sustava!

Još nismo riješili sljedeće:

- Koji mehanizam koristiti umjesto KBV?
- Kako se zaštititi od najezde čvorova koji žele poticaje?

Sybil napad

Obzirom da se svatko može pridružiti sustavu, isplativo je stvoriti puno klonova koji će samo skupljati poticaje.

Ključna ideja sustava Bitcoin: "Proof-of-work"

Čvor koji prvi riješi *kriptografsku slagalicu* predlaže sljedeći blok.

Poželjna svojstva kriptografske slagalice

- Rješenje slagalice ovisi o novom bloku (pa i cijelom lancu).
- Trivijalno je provjeriti je li rješenje slagalice ispravno.
- Za rješavanje slagalice je potrebno puno računalnih resursa.
- Kada puno čvorova pokušava riješiti slagalicu, šansa da će neki čvor A prvi pronaći rješenje je proporcionalna omjeru računalne snage čvora A i svih čvorova.

Novo pravilo: blok mora sadržavati rješenje hash slagalice

- Svaki blok sadrži proizvoljni broj *nonce*.
- Blok b se smatra *ispravnim* za *težinu* t ako vrijedi $H(b) < t$.

Rudarenje

Postupak rješavanja hash slagalica (odnosno naštimavanja broja *nonce* tako ta blok bude ispravan) u svrhu predlaganja novog bloka.

Ponavljanje: Hash funkcija H je korisna za slagalice

Ako je za svaki n-bitni *sažetak* y i za slučajno odabrani *prefix* k potrebno red veličine 2^n operacija kako bi se pronašao x takav da vrijedi $H(k||x) = y$ (dokle god k ima "dovoljno entropije").

Ako je hash funkcija H korisna za slagalice onda je najbolji mogući algoritam rudarenja ...

Za zadane transakcije $x_1, x_2, \ldots, x_m$ i *prag* t

1. Izaberi slučajan broj *nonce*.
2. Izračunaj $h = H(nonce|hash_{prev}|x_1|x_2|\ldots|x_m)$.
3. Ako je $h < t$ predloži blok, inače idi na početak.

Neka je fiksiran prag t i neka čvorovi $A_1, A_2, \ldots, A_k$ rudare tako da čvor A_i računa v_i sažetaka po sekundi. Neka sustav koristi hash funkciju H s n-bitnim sažetkom.

Zadatak

Koliko je očekivano vrijeme da čvor A_i riješi slagalicu?

Zadatak

Koliko je očekivano vrijeme da neki čvor predložiti novi blok?

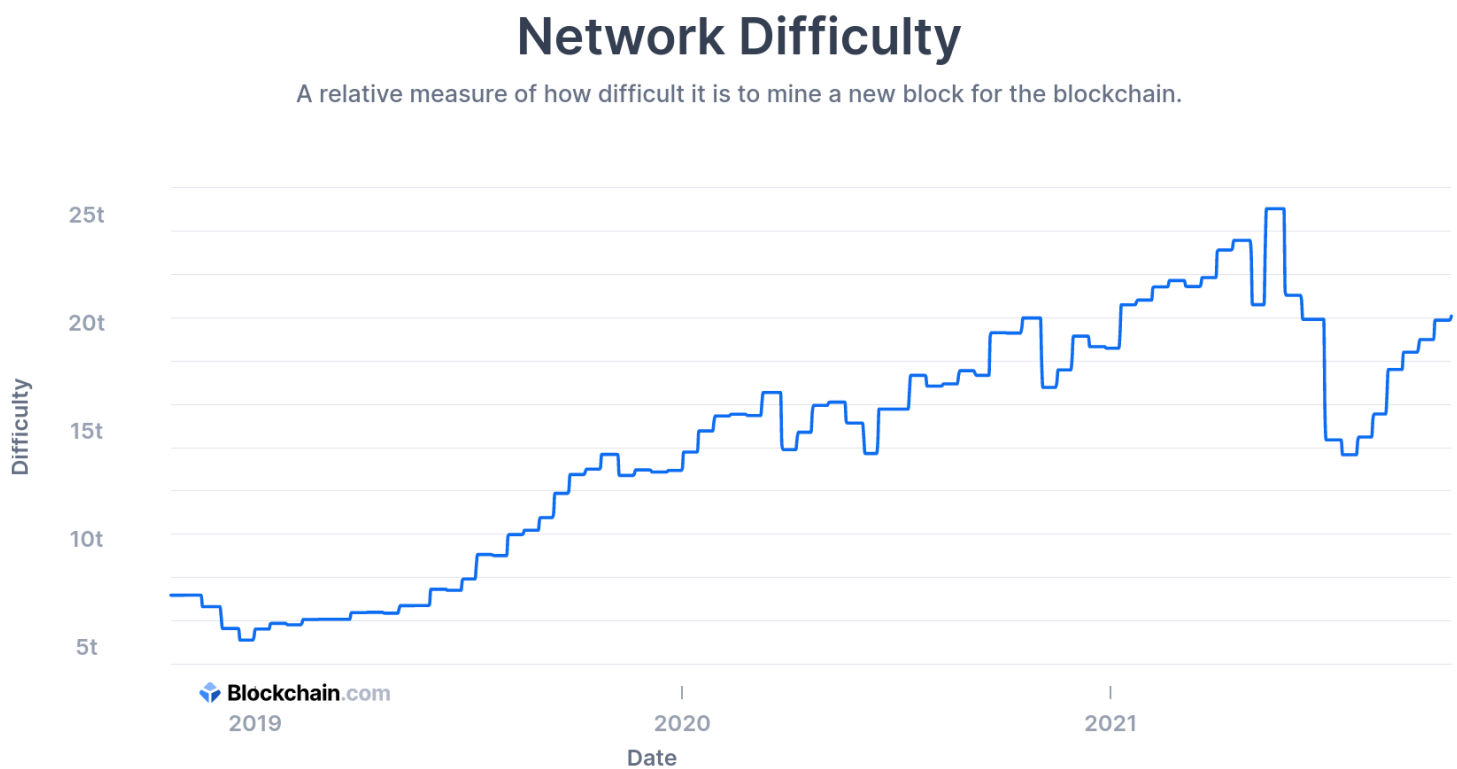
Zadatak

Koja je vjerojatnost da će čvor A_i prvi riješiti slagalicu i predložiti sljedeći blok.

Fakultet elektrotehnike i računarstva

Novo pravilo: podešavanje težine (Bitcoin)

Svakih 2016 blokova se prag t promijeni tako da je potrebno u prosjeku 10 minuta za novi blok.



Poticaji i “proof-of-work” su riješili sve naše probleme!

Dobili smo mehanizam biranja slučajnog bloka.

- Nemoguće je predvidjeti kojem će se bloku posrećiti da riješi slagalicu i predloži sljedeći blok.
- Ako ispravni čvorovi kontroliraju većinu računalnih resursa onda je vjerojatnost da je čvor koji predlaže sljedeći blok ispravan veća od pola.

Ne moramo uopće pretpostaviti da su čvorovi ispravni.

- Dovoljno je pretpostaviti da čvorovi djeluju sukladno vlastitim interesima.